DOCUMENTO REPORTE DE ACTIVIDAD
31 de mayo, 01 y 02 de junio de 2017

1. **Nombre del grupo de trabajo:**

   E-Justicia

   Subgrupo: Ciberdelincuencia
   Subgrupo: Ciberseguridad

2. **Grupo presencial / no presencial en Guatemala:**

   Subgrupo: Ciberseguridad

   Presencial y videoconferencia desde Uruguay y Ecuador

   Subgrupo: Ciberdelincuencia

   Presencial y videoconferencia desde Uruguay

3. **Resumen de la actividad realizada (indique brevemente cómo se ha desarrollado la actividad en la mesa, en el caso de ser un grupo presencial; o por otros medios en caso contrario):**

   Subgrupo Ciberseguridad

   Se utilizó el documento base propuesto y se hicieron las modificaciones, adiciones y adecuaciones para que el documento refleje lo que se ha conversado y sugerido por los distintos participantes. Se adjunta el documento generado.

   Se determinó que en la lista base solo se incluirán los recursos destinados específicamente a la protección de ciberataques. La lista por tanto quedó conformada por los siguientes recursos:

   - Firewall
   - Antimalware
   - Antispam
   - Análisis de vulnerabilidades
   - Prevención de intrusos
   - Administración de contenidos

- Correlación de eventos
- Auditorías internas y externas
- Recursos en línea
- Equipos de respuesta a incidentes (CSIRT)

Con base en esta lista de implementará un blog para compartirla con los especialistas de los países miembros y recibir sus aportes. Posteriormente se diseñará un instrumento de diagnóstico con características que fueron sugeridas en la discusión. Este instrumento permitirá realizar un análisis de brecha que ayudará a priorizar los temas de mayor interés para discusión en la red de cooperación.

En forma paralela debe buscarse un mecanismo de comunicación para la red que resulte ágil y funcional incluso en momentos en que se presente un incidente de seguridad. Este mecanismo permitirá el intercambio constante y permanente de información entre los especialistas en ciberseguridad de los países miembros. También facilitará la realización de actividades de capacitación.

Subgrupo: Ciberdelincuencia

Durante las sesiones celebradas del 31 de mayo de 2017, en el marco de la Segunda Ronda de Talleres, Antigua - Guatemala, el subgrupo de Ciberdelincuencia trabajó en el documento de "*Estudio de recomendaciones sobre Ciberdelincuencia*".

El objetivo de dicho documento consiste en elaborar un mapeo sobre el estado de las legislaciones de los países en relación con la Ciberdelincuencia.

Los objetivos específicos son:

Conocer la legislación de los países miembros de la Cumbre Judicial Iberoamericana, relacionada con los delitos informáticos, tanto en lo sustantivo como lo procesal.

Identificar Convenios Internacionales ratificados y/o en trámites de ratificación en los países miembros

.

Determinar Jurisprudencia relacionada con ciberdelincuencia en los países miembros.

1. Precisar la estructura organizativa en el marco de los delitos informáticos, donde se incluya la Policía Judicial, Ministerio Público y la Judicatura

En esta Ronda de Talleres se adoptaron los siguientes acuerdos:

1) Solicitar a los miembros la complementación del formulario para obtener los insumos necesarios para la realización del mapeo.
2) Elaborar el mapeo de cara a la III Ronda de Talleres que se llevará a cabo en Managua - Nicaragua

Elaboración de la guía:

A) Sub-Grupo de trabajo (Ciberdelincuencia) integrado por:

Costa Rica (Coordinadora)
Paraguay
Uruguay

Para la confección del documento se tiene como insumo el *"Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, Informe Ciberseguridad 2016"*,

4. Metodología de trabajo establecida para el desarrollo del proyecto (haga una breve exposición de la metodología de trabajo que se ha previsto para alcanzar los resultados previstos para el proyecto):

Subgrupo: Ciberseguridad

Se proyectó el documento base y con la participación de los integrantes se fueron discutiendo los puntos y se hicieron las modificaciones necesarias para adecuar el documento a la propuesta que se quiere hacer.

Se determinó que algunos de los recursos propuestos, si bien son importantes para la continuidad de los servicios, no son estrictamente recursos para ciberseguridad por lo que se incluyeron como anexo para que sean tomados en cuenta sin embargo no serán temas de discusión en la red de cooperación.

Se propuso la realización de un blog que estará a cargo de Costa Rica para socializar la lista y recibir los aportes de los especialistas de los países miembros. Este blog deberá desarrollarse durante el mes de junio para ser publicado en el mes de julio. Los aportes serán incorporados a la lista definitiva para que sea socializada durante el mes de agosto.

Esta lista servirá de base para la definición de un instrumento de diagnóstico que será tema de discusión del próximo taller.

Subgrupo: Ciberdelincuencia

A) Se discutió los principales puntos que debe contener el documento.
B) Se elaboró el formulario y documento final

Actividades y Plazos:

- El 05 de junio de 2017 se remite a las Secretarías Permanente y Pro-Tempore, el formulario a ser divulgado a todos los países miembros.
Responsable: Costa Rica

- Hasta el 31 de julio de 2017 los países miembros deben remitir el formulario, debidamente complementado a la coordinación del grupo de e-Justicia.

- Del 1 al 30 de agosto de 2017, elaboración del documento final con la información remitida por los países miembros.

5. Plan de trabajo acordado hasta la próxima convocatoria:

Subgrupo: Ciberseguridad

Crear un blog que permita la socialización de la lista propuesta para el mes de junio. El blog estará activo durante el mes de julio para recibir los aportes de especialistas de los países miembros. En el mes de agosto se incorporarán los aportes obtenidos del blog y se generará una lista definitiva que se socializará y servirá de base para que, en el próximo taller se defina la herramienta de diagnóstico.

Se sugiere que esta herramienta de diagnóstico sea implementada mediante una encuesta en línea. Con la información que genere esta encuesta se hará un análisis de brecha que permitirá determinar la prioridad de los temas a tratar en la red de cooperación. La idea es que los países con mayor avance en los temas priorizados cooperen con los que requieren apoyo para ir cerrando la brecha y lograr así un desarrollo uniforme en materia de ciberseguridad. Se propone que el análisis de brecha esté listo para la reunión preparatoria a realizarse en diciembre.

Subgrupo: Ciberdelincuencia

Se realizarán las siguientes actividades dentro de la metodología planteada:

- Ejecutar las acciones señaladas en el punto anterior.

- En la próxima ronda de talleres, se trabajará en afinar detalles y realizar las recomendaciones finales de este proyecto.

6. **Resultados alcanzados (exponga brevemente los principales resultados alcanzados para su grupo de trabajo en esta ronda de talleres):**

Subgrupo: Ciberseguridad

Se definió el proceso básico que se seguirá para la implementación de la red de cooperación en materia de ciberseguridad y se propuso una lista base de los temas que serán tratados en dicha red.

Subgrupo: Ciberdelincuencia

Se intercambiaron criterios en torno al fenómeno de la ciberdelincuencia y se definió la necesidad de contar mayor información, para conocer en qué nivel de desarrollo normativo se encuentra cada país.

Se realizó el documento base para la recolección de los datos necesarios para alcanzar los objetivos planteados.

Se estableció la agenda de trabajo de cara a la próxima ronda de talleres, a realizarse en el mes de setiembre en Managua, Nicaragua.

7. **Desviaciones importantes del proyecto original (si han propuesto desviaciones importantes respecto de los objetivos o resultados del proyecto original, por favor indíquelas y razone los motivos de las mismas):**

Subgrupo: Ciberseguridad

No se proponen desviaciones importantes de la propuesta original

Subgrupo: Ciberdelincuencia

No existen desviaciones

8. **Documentos de trabajo que se adjuntan: (por favor haga una relación de los documentos de trabajo resultantes de esta ronda y que son entregados en formato digital a la Secretaría Permanente; para ser incluidos en la web de Cumbre, página correspondiente a los grupos de trabajo):**

Subgrupo: Ciberseguridad

Se anexa el documento generado con la propuesta y la lista base de temas que serán incluidos en el blog

Subgrupo: Ciberdelincuencia

Se anexa el documento "*Estudio de recomendaciones sobre Ciberdelincuencia*" para ser distribuido para el levantamiento de la información, entre los países miembros de Cumbre Judicial.

9. **Nombre, cargo y país de las personas que han participado en el grupo de trabajo:**

No.	NOMBRE	CARGO	PAÍS
Ciberseguridad Presencial			
1.	Luis Guillermo Rivas Loáiciga	Magistrado	Costa Rica
2.	Orlando Castrillo Vargas	Subdirector TI	Costa Rica
3.	Luis Eduardo Yepes Gómez	Unidad Informática de la Rama Judicial	Colombia
4.	Martín Antonio García Díaz	Director General de Tecnologías de la Información y Comunicaciones	Nicaragua
Videoconferencia			
5.	Gustavo Castillo	Gerente de Proyectos de la Dirección Nacional de Tecnologías de la Información y Comunicación	Ecuador

No.	NOMBRE	CARGO	PAÍS
6.	Luis Marcelo Pesce Rami	Subdirector General de los Servicios Administrativos del Poder Judicial	Uruguay
Ciberdelicuencia Presencial			
7.	Paublino Escobar Garay	Juez Penal	Paraguay
8.	Patricia Bonilla Rodríguez	Asistente de Presidencia Corte Suprema de Justicia	Costa Rica
Videoconferencia			
9.	John Pérez Brignani	Ministro de Tribunal	Uruguay
Participación			
10.	Kattia Morales Navarro	Directora de Tecnología	Costa Rica

10. Nombre, cargo y país del coordinador o coordinadores del Grupo de Trabajo:

No.	NOMBRE	CARGO	PAÍS
1.	Luis Guillermo Rivas Loáiciga	Magistrado	Costa Rica

11. Sugerencias para la siguiente reunión:

Ciberseguridad y Ciberdelincuencia

- Para la siguiente reunión se propone el diseño del instrumento que servirá para el diagnóstico con base en las características que fueron sugeridas. Se sugiere que, una vez establecida la lista definitiva de temas que serán tratados en la red de cooperación se solicite a los especialistas de los países miembros aportes sobre las preguntas que deberían incluirse en ese instrumento en forma previa al taller, de tal forma que se cuente con una propuesta base sobre la cual trabajar en el taller.

- Retomar la inclusión de Ministros o Magistrados afines con temas tecnológicos de los diferentes países de Cumbre Judicial Iberoamericana por cuanto su participación fortalecerá los objetivos actuales y futuros de éste grupo de trabajo.

- Realizar un seminario de E Justicia donde participen por cada uno de los países al menos, un representante técnico y un Magistrado Ministro, donde de forma amplia cada país pueda exponer sus experiencias en materia de tecnología así como otras sugerencias donde se expongan por parte de organizaciones el uso de la tecnología en el proceso judicial, sin que esta iniciativa sustituya la feria de tecnología que se realiza en cada asamblea plenaria.

- Se insta a cada país a promover a lo interno ferias de tecnología que involucren a otras instituciones del Estado y al propio personal de tecnología de cada institución.

- Tener en cuenta que para efectos del Reglamento de la posible comisión se estima que la misma no debe contener un número limitado de participantes, que sea abierto y que si quieren participar los 23 países puedan incorporarse.

ESTUDIO DE RECOMENDACIONES SOBRE CIBERDELINCUENCIA

La "*Evolución Tecnológica*", ha transformado el mundo y la forma en que las personas realizamos las diferentes actividades sean cotidianas, económicas, académicas, de servicios, comunicación, producción, entre otros.

Dicha evolución, también ha incidido en la forma en que se realizan las actividades delictivas, donde la tecnología es utilizada como "*medio*" para cometer delitos comunes y de crimen organizado, o bien, como "*objeto*" de la actividad delictiva.

El delito informático ha sido definido como aquella "*acción delictiva que realiza una persona, con la utilización de un medio informático o lesionando los derechos del titular de un elemento informático, se trate de máquinas -hardware- o de los programas – software*"[1]

Los delitos informáticos tiene como características que: a) son de rápida ejecución y alto alcance, b) de fácil encubrimiento, c) novedosos, d) no siempre son fáciles de tipificar, e) generan nuevos bienes jurídicos tutelados, f) son intangibles, g) difíciles de vigilar, h) transitorios por su naturaleza, i) pueden ser disociados en el tiempo, j) difícil identificación del autor, por lo tanto, son difíciles de investigar, perseguir y juzgar.

La ciberdelincuencia, es una amenaza que si bien es cierto actúa de forma silenciosa, el daño es de gran impacto, generando pérdidas a nivel mundial, siendo que, durante el año 2016, de acuerdo con estudios realizados, se estima que el total de costos financieros

[1] Chinchilla Sandí, Carlos. (2004) Delitos Informáticos: Elementos básicos para identificarlos y su aplicación. San José, Costa Rica. Ediciones Farben

Si bien es cierto, el estudio realizado por la OEA, no hace relación al sistema jurisdiccional propiamente dicho, el mismo sirve de base, para tener una visión global de la situación actual de algunos de los países miembros, puesto que, no se abarca a los países ibéricos.

Ahora bien, en relación con el "***Derecho Penal Sustantivo***", cada uno de los niveles se valora de la siguiente manera:

1: *"El derecho penal sustantivo específico para la delincuencia cibernética no existe, o existe el derecho penal general y se aplica ad hoc a la delincuencia cibernética".*

2: *"Existe una legislación parcial en el derecho penal sustantivo que aplica los marcos legales y regulatorios a algunos aspectos de los delitos cibernéticos; está siendo discutido el derecho penal sustantivo para la delincuencia cibernética entre los legisladores, pero ha comenzado el desarrollo de la ley".*

3: *"La legislación vigente tipifica una serie de delitos relacionados con pruebas electrónicas que pueden ser objeto de una legislación específica o abordados en el código penal".*

4: *"El país se adhiere a las mejores prácticas y normativas regionales e internacionales pertinentes sobre derecho de delito cibernético y asigna los recursos de acuerdo a las prioridades nacionales".*

5: *"El país continuamente busca incluir el desarrollo de las mejores prácticas internacionales sobre delito cibernético en la legislación nacional y es un colaborador activo en el discurso global sobre la mejora de los instrumentos de la lucha contra delitos cibernéticos internacionales; existen medidas para superar en el país las líneas de base mínimas de seguridad internacional".*

causados por la ciberdelincuencia durante dicho año, supera los US$125.900 millones de dólares.[2]

Las tendencias futuras en el incremento del cibercrimen, están orientadas a actividades como : el "*Crime-as-a-Service*", "*Ransomware*", "*Uso criminal de datos*", "*Fraude de pago*", "*Abuso sexual infantil en línea*", "*Abuso de la Darkenet*", "*Ingeniería Social*",

"*Monedas Virtuales*"[3], así como el ataque a infraestructuras críticas, lo cual pone en peligro vidas humanas y la economía de los países.

Estudios han señalado que los marcos jurídicos relacionados con la ciberseguridad y la ciberdelincuencia, de los diversos países de la región se encuentran aún en una etapa incipiente, en cuanto a la promulgación de leyes relacionadas con la materia.

A continuación, se presenta un cuadro referente a la situación de cada país, cuyos datos fueron extraídos del informe denominado *"Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, Informe Ciberseguridad 2016"*, realizado por el Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID).

Dicho estudio realiza una evaluación, donde identificaron cinco niveles de madurez de la capacidad de seguridad cibernética en Latinoamérica, a saber: "*Inicial*", "*Formativo*", "*Establecido*", "*Estratégico*" y "*Dinámico*". Para efectos del cuadro, se representarán con los valores: 1, 2, 3, 4 y 5, respetivamente.

---

[2] Informe Norton Ciberseguridad 2016 recuperado el 30-May-2017 en https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf

[3] http://www.ituser.es/seguridad/2016/10/europol-presenta-su-informe-sobre-el-cibercrimen-en-europa

En cuanto al "***Derecho procesal de delincuencia cibernética***", los niveles valoran lo siguiente:

1: *"No existe el derecho penal procesal adecuado para la delincuencia cibernética y el uso de la prueba electrónica en otros crímenes, o existe el derecho penal procesal general y se aplica ad hoc a la delincuencia cibernética y al uso de la prueba electrónica en otros crímenes".*

2: *"Se está discutiendo y desarrollando el derecho procesal penal en relación con la prueba electrónica; el derecho procesal penal se aplica ad hoc a la delincuencia cibernética, pero no ha comenzado el desarrollo de los delitos cibernéticos específicos".*

3: *"Se ha implementado el derecho procesal penal integral y los requisitos probatorios relacionados; las mejores prácticas se emplean por aplicación de la ley en el ejercicio de poderes procesales".*

4: *"En el caso de la investigación transfronteriza, el derecho procesal estipula las acciones que es necesario realizar bajo las características de casos particulares, con el fin de obtener con éxito la prueba electrónica".*

5: *"El país se adhiere a las mejores prácticas internacionales sobre procedimiento penal de delito cibernético y la obtención de pruebas electrónicas, y constantemente busca implementar estas medidas en la legislación nacional y sirve como un colaborador activo en el discurso global sobre la mejora de la lucha contra los delitos cibernéticos internacionales; existen medidas para superar las líneas de base mínimas de seguridad internacional, que contribuyen al desarrollo de mejores prácticas internacionales".*

Y en lo que se refiere al "***Cumplimiento de la ley***", el estudio señala que:

1: *"No existe la capacidad de las autoridades policiales para prevenir y combatir los delitos relacionados con la cibernética".*

2: *"Existe alguna capacidad de investigación para indagar delitos que involucren pruebas electrónicas, así como para obtener dichas pruebas, de conformidad con el derecho interno; sin embargo, esta capacidad es mínima".*

3: *"Se ha establecido una capacidad institucional integral para investigar y manejar casos de delincuencia cibernética y delitos relacionados con pruebas electrónicas, incluyendo los recursos humanos, procesales y tecnológicos, medidas exhaustivas de investigación, cadena de custodia digital y gestión de integridad de las pruebas y mecanismos formales e informales de colaboración con interesados internacionales y nacionales (actores de los sectores privado y público)".*

4: *"Los oficiales de las fuerzas de la ley reciben una formación continua basada en las responsabilidades relativas y en entornos de amenazas nuevas y cambiantes y pueden utilizar herramientas forenses digitales sofisticadas para investigar delitos informáticos complejos y delitos relacionados con pruebas electrónicas; los organismos locales de aplicación de la ley colaboran con contrapartes regionales e internacionales en investigaciones".*

5: *"Existen recursos dedicados a unidades de delitos informáticos plenamente operativas, incluyendo capacidades avanzadas de investigación y de gestión de integridad de los datos; es posible recoger y analizar las estadísticas y tendencias que mejorarían la investigación sobre los delincuentes con el fin de facilitar una comprensión exhaustiva del ambiente delictivo en línea y contribuir a la toma de*

decisiones estratégicas; las agencias de aplicación de la ley nacionales están participando plenamente en la investigación y redes transfronterizas".

País	Derecho sustantivo de delincuencia cibernética	Derecho procesal de delincuencia cibernética	Cumplimiento de la ley
Argentina	3	3	3
Bolivia	2	2	2
Brasil	3	4	4
Chile	3	4	3
Colombia	3	3	3
Costa Rica	3	3	3
Ecuador	3	2	2
El Salvador	2	2	2
Guatemala	2	1	2
Honduras	2	1	1
México	3	2	4
Nicaragua	1	3	1
Panamá	3	2	2
Paraguay	3	2	2

Perú	3	2	2
República Dominicana	5	5	5
Uruguay	1	2	2
Venezuela	3	1	2

Para conocer cuál es la situación real de cada país, en relación con su legislación referente a los delitos informáticos, se considera oportuno realizar un estudio a través de una matriz, donde se especificarán los tipos penales, leyes especiales o procesales de sus legislaciones, así como la estructura organizativa, jurisprudencia y convenios suscritos por sus respectivos estados.

A partir de este estudio de campo, se podrá precisar el estado en que se encuentra cada país, en relación a este tipo de hechos punibles, y a partir de allí dictar recomendaciones, o bien, este podrá ser de utilidad para cada uno a efecto de que tomen las precauciones y realicen las iniciativas que consideren oportunas, para armonizar sus legislaciones conforme a los nuevos estándares internacionales.

Un aspecto importante a considerar, es que en la medida que los países tengan armonizada la normativa jurídica, con el resto de la región, la misma, facilitará mayor cooperación internacional, con el fin de perseguir y castigar a los partícipes de este tipo de hechos, y consecuentemente facilitar la extradición tanto activa, como pasiva, de este tipo de conductas al margen de la ley.

Es por lo anterior que se recomienda a los países miembros de la Cumbre Judicial Iberoamericana, promover los mecanismos jurídicos, procesales y de cooperación

internacional, que faciliten la lucha contra este tipo de criminalidad, razón por la cual, se presenta el siguiente informe, el cual muestra un catálogo de tipos penales, utilizados en los diferentes países para sancionar conductas delictivas relacionadas con el ciber-crimen.

ESTUDIO NORMATIVO RELACIONADO CON EL CIBERCRIMEN

Se solicita a cada uno de los países de Cumbre Judicial, llenar el siguiente formulario, el cual nos permitirá obtener los insumos necesarios, para precisar las normas que regulan los delitos determinantes o que se refieran al ciber-crimen, así como, jurisprudencia relacionada y la estructura organizacional de las instituciones involucradas en este tipo de actividades ilícitas.

El documento se ha dividido en cuatro puntos:

I. Legislación de los países miembros de la Cumbre Judicial Iberoamericana, relacionada con los delitos informáticos

II. Convenios Internacionales ratificados y/o en trámites de ratificación en los países miembros.

III. Jurisprudencia relacionada con ciberdelincuencia en los países miembros.

IV. Estructura organizativa en el marco de los delitos informáticos, donde se incluya la Policía Judicial, Ministerio Público y la Judicatura

El presente formulario tiene como objetivo elaborar un mapeo sobre el estado de las legislaciones de los países en relación con la Ciberdelincuencia.

I. LEGISLACIÓN DE LOS PAÍSES MIEMBROS DE LA CUMBRE JUDICIAL IBEROAMERICANA, RELACIONADA CON LOS DELITOS INFORMÁTICOS

Este apartado se ha divido en dos áreas: normas sustantivas y normas procesales. Para complementar los datos, la tabla se divide en cinco columnas, a saber:

a) **Tipo penal de referencia:** En esta columna se presentan algunos tipos penales que se encuentran incorporados en el derecho positivo. El dato allí señalado, debe considerarse sólo como referencia, por cuanto, el "*nom iuris*" en cada país podría variar.
b) **Artículo:** Se debe anotar el número del artículo
c) **Cuerpo normativo:** Nombre del cuerpo normativo donde se encuentra tipificada la norma
d) **Nombre de la norma:** "*Nom iuris*" conforme a la legislación del país estudiado
e) **Descripción del tipo penal:** Descripción literal del tipo penal

Además, es importante destacar que los tipos penales de referencia aquí anotados, son una guía, no obstante, cada país puede incorporar aquellos que tengan en su legislación y que no se encuentren aquí señalados.

FORMULARIO
ESTADO ACTUAL DE LA CIBERDELINCUENCIA EN LOS PAÍSES DE CUMBRE JUDICIAL IBEROAMERICANA

País: _____

Nombre contacto del país: _____

Correo electrónico: _____

- Normas jurídicas sustantivas relacionadas con ciberdelincuencia

Tipo Penal de referencia	Artículo	Norma	Nombre de la norma (conforme a su legislación)	Texto de la norma
DELITO INFORMÁTICO COMO MEDIO DE LA ACCIÓN DELICTIVA				
Delitos Sexuales				
Corrupción				
Seducción o encuentros con menores por medios electrónicos (Grooming)				
Turismo sexual				
Fabricación, producción o reproducción de pornografía				
Pornografía virtual y pseudo pornografía				
Tenencia de material pornográfico				

Difusión de pornografía

Delitos contra el ámbito de intimidad

Violación de correspondencia o comunicaciones	
Violación de datos personales.	

Delitos contra la propiedad

Extorsión informática (Ransomware)	
Estafa informática	
Daño agravado	
Narcotráfico y crimen organizado	
Espionaje	

DELITO INFORMÁTICO COMO OBJETO DE LA ACCIÓN DELICTIVA

Delitos informáticos y conexos

Sabotaje informático
Daño informático
Suplantación de identidad
Espionaje informático
Instalación o propagación de programas informáticos maliciosos
Suplantación de páginas electrónicas
Facilitación del delito informático
Difusión de información falsa

- **Normas jurídicas procesales relacionadas con ciberdelincuencia**

Norma procesal de referencia	Artículo	Cuerpo normativo	Nombre de la norma (conforme a su legislación)	Descripción de la norma procesal penal

II. CONVENIOS INTERNACIONALES RATIFICADOS Y/O EN TRÁMITES DE RATIFICACIÓN

Indicar aquellos convenios internacionales ratificados, o en proceso de ratificación, en su país.

a) **Nombre convenio:** Señalar el nombre del convenio
b) **Estado:** Se refiere si el mismo está ratificado, o bien, se encuentra en pendiente o en proceso de ratificación
c) **Fecha de promulgación:** En caso de estar ratificado, indicar la fecha de promulgación
d) **Fecha de ratificación:** Señalar la fecha de ratificación en su país

Nombre Convenio	Estado	Fecha de promulgación	Fecha de ratificación

III. JURISPRUDENCIA RELACIONADA CON CIBERDELINCUENCIA

Con el fin de obtener información de criterios jurisprudenciales de los diversos países, se considera oportuno, obtener las resoluciones emitidas por los altos tribunales (Tribunales o Sala de Casación), relacionados con los delitos informáticos

a) **Tribunales de Apelación o Sala de Casación:** Indicar el nombre órgano que dicta la resolución
b) **No. Voto o Sentencia:** Anotar el número de voto o sentencia, que la identifique
c) **Fecha:** Fecha de emisión del voto o sentencia
d) **Tipo Penal:** Indicar el tipo penal que fue objeto de discusión en el recurso
e) **Nombre documento adjunto:** Indicar el nombre del documento que se adjunta a este formulario con el contenido del voto o sentencia señalado.

Tribunal de Apelación o Sala de Casación	No. Voto	Fecha	Tipo penal	Nombre documento adjunto

IV. ESTRUCTURA ORGANIZATIVA EN EL MARCO DE LOS DELITOS INFORMÁTICOS

Con el fin de conocer la estructura organizativa de cada Institución, relacionada con los delitos informáticos, se considera oportuno conocer, si en los países miembros, se cuenta con unidades de especialización creadas para investigar, combatir y judicializar, los hechos punibles cometidos a través del uso de la tecnología informática, desde la investigación, recolección, manejo de evidencia y prueba digital, entre otros. Por ejemplo, si existen Fiscalías, Unidades de la Policía o Jurisdicciones especializadas en Delitos Informáticos.

En caso de no existir unidades especializadas, indicar cuál es la estructura utilizada.

a) **Institución:** Nombre de la oficina
b) **Funciones:** Indicar las funciones que realiza dicha unidad

Institución	Funciones
Policía Judicial	
Ministerio Público	
Judicatura	

Estudio de recomendaciones sobre Ciberseguridad

Introducción

La seguridad informática busca garantizar la consistencia, integridad y confiabilidad de la información que se gestione a través de medios tecnológicos.

Se parte de la premisa de que no existe la seguridad informática al 100%. Bajo esta óptica, podemos dividir los esfuerzos en esta materia en dos tipos: los que van orientados a mantener la continuidad de los servicios y los que van orientados a recuperarse en el caso en que, a pesar de todos los esfuerzos realizados, se haya presentado una interrupción en los servicios.

El gasto en seguridad informática tiene un comportamiento asintótico con respecto a la mejora que se obtiene al incrementar la inversión en tecnología. Al principio se pueden realizar mejoras muy importantes con poca inversión, pero conforme se avanza las mejoras que se obtienen son cada vez menores y para obtenerlas se requiere un mayor gasto.

Por más esfuerzo que se haga, aún la organización con mayor capital y mayores recursos tendrá aspectos susceptibles de mejora. El límite del gasto que se realiza en esta materia se define con base en una valoración costo – beneficio y en una adecuada administración de riesgos.

El aprovechamiento de los recursos se vuelve por tanto un factor crítico. Sin embargo en la actualidad es posible que los países miembros de cumbre efectúen las mismas pruebas y hasta cometan los mismos errores porque no están compartiendo información.

Se propone la creación de una red de cooperación en materia de ciberseguridad entre los países miembros de la Cumbre Judicial Iberoamericana. La finalidad de esta red es crear un medio para que los especialistas en la materia de los diferentes países puedan compartir las mejores prácticas generando así una sinergia que evite, en la medida de lo posible, el desgaste de esfuerzos y que facilite la cooperación entre los miembros, y la socialización de experiencias con el fin de uniformar la fortaleza ante las amenazas cibernéticas.

Existen diferentes factores que forman parte de los esfuerzos que las organizaciones deben realizar para garantizar la continuidad de los servicios. En el Anexo #1 se listarán estos servicios con la finalidad de que sean considerados sin embargo no serán tratados en la red de cooperación propuesta.

Se presentará a continuación una breve descripción de los aspectos que serán tema de discusión de la red de cooperación. Este listado será socializado con los países miembros para incorporar sus aportes.

La siguiente etapa del proceso será la realización de un diagnóstico, mediante un instrumento idóneo, que permita a cada país determinar los aspectos susceptibles de mejora y los países que podrían colaborar en el proceso.

Recursos específicos para repeler ataques cibernéticos

Los siguientes aspectos serán de interés y discusión en la red de cooperación.

Cultura organizacional

El primer elemento de un esquema de seguridad informática es la cultura de los usuarios. Ningún esquema de seguridad, por más fuerte que sea puede compensar los descuidos y faltas que puedan tener los usuarios. Si los usuarios insisten en abrir correos maliciosos, ingresar a sitios dudosos o utilizar software ilegal, no hay forma de cerrar todos los portillos existentes por lo que mediante estas acciones pondrán en riesgo la seguridad informática de la organización.

Se requiere por tanto que se defina en primera instancia un marco de control, compuesto por políticas, procedimientos, reglamentos y sanciones apoyados y aprobados por la administración superior de la organización.

Pero además se requiere instruir al usuario en temas de seguridad informática de tal forma que tenga los elementos para valorar los riesgos a que se enfrenta y las posibles consecuencias de sus actos. Esto puede realizarse mediante diferentes formas tales como campañas de información sobre diferentes temas y cursos específicos.

Sin temor a equivocarse los esfuerzos que se realicen en estos temas cubren más del 50% del trabajo que implica la seguridad informática de la organización y la inversión requerida para su implementación es relativamente baja.

Elementos del esquema de seguridad informática

Además de la seguridad que se puede implementar propiamente con los componentes de la plataforma tecnológica de la institución (ver Anexo #1) existen una serie de recursos que se adicionan específicamente para solventar debilidades en materia de seguridad informática. Algunos de estos recursos resultan onerosos para muchas organizaciones sin embargo debe valorarse su uso, aún y cuando se limite a áreas muy críticas de la plataforma. También deben considerarse opciones de software libre. Entre estos recursos se puede mencionar:

- Firewall: Estos dispositivos, también conocidos como paredes de fuego, trabajan por denegación por omisión, es decir, lo que no está expresamente autorizado está denegado. Se utilizan para controlar el flujo de información entre dos redes o segmentos de estas. Existen firewalls que trabajan en capas 3 y 4 y otros que trabajan a nivel de aplicación en la capa 7 del modelo OSI. La gama de opciones para un dispositivo de este tipo va desde uno hecho con una PC con dos o más tarjetas de red y una distribución de Linux hasta los más sofisticados que reconocen mediante inteligencia artificial posibles ataques y los repelen. Algunos tienen, previo contrato de servicio, conexión con el fabricante para que este alimente y actualice las firmas (patrones de ataques que reconoce el dispositivo) y las diferentes listas de sitios potencialmente peligrosos para que el administrador defina si se bloquea o se permite el acceso a esos sitios. El fin último de un firewall es permitir el tráfico estrictamente necesario y su efectividad estará en relación directa con la habilidad de su administrador.

- Antimalware: Los delincuentes informáticos generan software que, una vez que ha ingresado en la organización, puede ejecutar diferentes acciones, desde borrar información hasta dar acceso al hacker para que tome control del equipo en que se instaló. Para evitar este riesgo existen productos que se encargan de revisar en cada equipo de la plataforma el software que ingresa. Para que este esquema sea efectivo el software debe estarse actualizando constantemente para incorporar las nuevas amenazas que van surgiendo y para incorporar mejoras a su funcionamiento y efectividad. Estos productos consumen un porcentaje importante de la capacidad de cómputo de los equipos y también tienen un consumo significativo de ancho de banda en la red por lo que su correcta administración resulta crucial para que se constituyan en una solución y no en un problema.

- Antispam: Mención aparte merece el recurso que se encarga de evitar que ingrese correo basura a la organización. Este correo es molesto, consume recursos de red, de almacenamiento y de procesamiento y podrían presentar patrones virales que lo faculten a reproducirse con lo cual se agravan los problemas indicados y además se compromete la credibilidad de la organización al convertirla en fuente de correos indeseados. Sirven además como transporte de otras formas de malware lo que los hace doblemente peligrosos.

- Análisis de vulnerabilidades: Los diferentes productos de software que se instalan en los equipos que componen la plataforma de la organización no son perfectos. Con el paso del tiempo se detectan fallos que los delincuentes informáticos pueden utilizar para sobrepasar los mecanismos de seguridad que se hayan establecido. Estos fallos se conocen como vulnerabilidades. Encontrar y reparar estas vulnerabilidades es una labor titánica por lo que se han desarrollado productos que buscan, con base en la información que publican los distintos fabricantes, estas vulnerabilidades y las informan a tiempo junto con una recomendación para su reparación de tal forma que se hace posible mantener el nivel de vulnerabilidad de los equipos en un rango aceptable. Estos productos deben complementarse con servicios de instalación automatizada de los parches que solventan las deficiencias encontradas.

- Prevención de intrusos: Dado que no se puede asumir que los esquemas de seguridad, en ningún caso, son impenetrables, siempre existe la posibilidad de que un delincuente informático vulnere esas defensas y logre llegar hasta los dispositivos críticos de la organización. Los sistemas de prevención de intrusos contemplan esta posibilidad e incorporan mecanismos para detectar y repeler el acceso de intrusos a los dispositivos clave.

- Administrador de contenidos: A pesar de las advertencias y capacitaciones los usuarios podrían por alguna razón terminar tratando de ingresar a un sitio en internet inadecuado, ya sea por su contenido o porque representa un riesgo potencial para la seguridad informática de la organización. Mediante la administración de contenidos los sitios que se pueden accesar se pueden limitar conforme a las políticas organizaciones evitando riesgos y pérdida de tiempo laboral.

- Correlación de eventos: La mayoría de los dispositivos de la plataforma tecnológica de la organización generan eventos que en forma aislada podrían no dar mayor información pero que si se correlacionan con los que generan otros dispositivos podrían indicar la materialización de algún riesgo. Este tipo de productos buscan recolectar los eventos que generan los distintos dispositivos y realizar una correlación para determinar comportamientos que de otra forma pasarían inadvertidos.

- Auditorías internas y externas en materia de seguridad informática: El esfuerzo por detectar y corregir debilidades debe ser constante. Bajo esta premisa es importante contar con personal especializado a lo interno que realice diferentes estudios e intentos controlados de intrusión con el fin de eliminar los portillos que pudieran utilizar los delincuentes informáticos antes de que estos los encuentren. También se debe contratar, al menos una vez al año, este tipo de revisión por parte de un tercero experto con un enfoque diferente.

- Recursos en línea: Existen numerosos recursos en línea que pueden utilizarse para mejorar la seguridad informática. Tal es el caso del servicio de revisión de páginas web que provee la fundación OWASP (www.owasp.org) o el escaneo de metadatos que ofrece el sitio www.elevenpaths.com mediante su aplicación FOCA. Si bien es cierto no se puede hacer uso de cualquier página, existen servicios como los mencionados que brindan un aporte significativo.

- CSIRT: Dado que no existe garantía de que no se presenten incidentes, la organización debe estar preparada para actuar en estos casos. Un CSIRT es un equipo de respuesta a incidentes, el cual sabe de antemano como se debe actuar en estas situaciones. Este equipo monitorea además las alertas a nivel mundial con la finalidad de prevenir la ocurrencia de incidentes conocidos y mantiene además comunicación con otros equipos similares a nivel mundial con fines de mutua cooperación.

Socialización de los temas de interés

La lista de los temas de interés se va a socializar con todos los países miembros para que sus especialistas puedan hacer aportes. Con la incorporación de los aportes se generará una lista definitiva que se hará de conocimiento de los países miembros.

Se propone el uso de un blog en el que se publicará la lista base que se propone en este documento y se dará un tiempo prudencial para la discusión y definición.

Costa Rica propone hacerse cargo de la implementación de este blog.

Características del instrumento que se definirá

Con base en la lista de los temas que se incluyan como de interés de la red de cooperación se realizará un diagnóstico que permita determinar el nivel de seguridad, de cada país, en cada uno de los aspectos incluidos.

Se propone para este fin la utilización de una encuesta en línea que, en la medida de lo posible, deberá respetar los siguientes parámetros:

- Deberá ser fácil de llenar y tomar el menor tiempo posible
- Deberá respetar la independencia y confidencialidad de los países miembros
- Deberá utilizar una escala que permita la comparación entre los diferentes países

Costa Rica propone hacerse cargo de la implementación de la encuesta en línea.

Análisis de Brecha

El diagnóstico servirá de base para iniciar un proceso de colaboración entre los países miembros en el que, con base en las diferencias encontradas, se definirá la forma en que se minimizará la brecha existente.

Se propone que se definan y prioricen los temas de mayor interés y se busquen mecanismos para compensar las deficiencias. Estos mecanismos van desde la asesoría del país que mayor desarrollo tiene en un tema a los demás hasta la contratación por parte de alguno de los países de un especialista y la posterior replicación del conocimiento y la experiencia a los demás.

Colaboración

Conforme las experiencias positivas y el flujo de información lo permitan, los participantes podrán tener discusiones respecto a las mejoras que se requieren para enfrentar los diferentes retos que presentará el futuro. Se compartirá información respecto al comportamiento de amenazas a nivel mundial y los mecanismos más efectivos para enfrentarlas.

Se espera además que los especialistas puedan realizar investigaciones conjuntas, acordar temas de interés y preparar capacitaciones de unos a otros y que se apoyen cuando alguno tenga un incidente de seguridad que atender.

Mecanismos de integración de la red de cooperación en ciberseguridad

Uno de los principales temas que debe definirse en el proceso de implementación de la red de cooperación es el mecanismo que utilizarán los especialistas para comunicarse en forma efectiva.

Debe ser un medio que permita compartir distintos tipos de información (texto, audio, video) y de preferencia debe tener a los miembros en línea permanentemente.

Se deberá definir también un protocolo para el uso de este medio de comunicación que permita su mejor aprovechamiento.

Conclusiones

El problema de la seguridad informática es común a todos los miembros y todos estamos expuestos a las mismas amenazas por lo que resulta lógico conformar una red de cooperación en materia de ciberseguridad que permita compartir conocimientos y experiencias con que se podrá definir la mejor línea de acción conocida.

Se propone por tanto la conformación de una red de cooperación en materia de ciberseguridad conformada por los especialistas de los países miembros.

Para este fin se propone una lista base de temas que serán considerados de interés para las discusiones de la red de cooperación. Esta lista será socializada mediante un blog que será implementado por Costa Rica. Se dará un tiempo prudencial para recibir aportes. Con base en los aportes de los países miembros se conformará una lista definitiva.

A partir de esta lista se desarrollará una encuesta electrónica que permita el diagnóstico de la situación actual en materia de ciberseguridad de los países miembros.

Este diagnóstico permitirá un análisis de brecha que posibilitará la definición y priorización de los temas que serán abordados inicialmente en la red de cooperación.

La finalidad última de la propuesta es implementar un flujo constante y efectivo de información en materia de ciberseguridad que permita a los especialistas de los países miembros actuar como un solo equipo generando así sinergia.

Para tal fin se requiere de la definición de los mecanismos de comunicación apropiados para este fin y de los correspondientes protocolos para la correcta utilización de estos canales.

Se propone la definición de la lista base definitiva para el siguiente taller preparatorio el cual servirá de base para definir el instrumento de diagnóstico en ese taller. Para este fin se deberá implementar el blog en el mes de junio, permitir la discusión y la incorporación de aportes para el mes de julio. La confección y distribución de la lista definitiva se daría en el mes de agosto.

Anexo #1

Temas que no serán de discusión en la red de cooperación

Marcos de control

En primer lugar es menester indicar que existen múltiples normas, estándares y buenas prácticas que ayudan a ordenar los esfuerzos que se requieren para tener un adecuado control y gobierno de las tecnologías de la información. Es recomendable por tanto aprovechar estos marcos entre los que se pueden citar dos de los más importantes, la familia 27000 de ISO (http://www.iso27000.es/iso27000.html) y el marco de control COBIT en su última versión (http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx).

Seguridad física

Este aparte se refiere a elementos que, sin ser específicamente parte de la plataforma tecnológica, resulta de suma importancia para el funcionamiento de esta. Entre los elementos que se pueden mencionar están:

- Red eléctrica: Los equipos que componen la plataforma tecnológica requieren de energía eléctrica para su funcionamiento. Esta energía debe tener los niveles de calidad establecidos por los fabricantes para que los dispositivos no fallen. Pero además se requiere que el diseño de la red eléctrica soporte los equipos que se van a instalar en cada lugar, se requiere un adecuado sistema de tierras que tal forma que la electricidad sobrante se deseche por los canales apropiados y se requiere que la alimentación eléctrica sea continua lo cual implica la necesidad de contar con sistemas de UPSs y plantas eléctricas que den continuidad al servicio en caso de algún corte en el fluido eléctrico.

- Sistemas de control ambiental: Los equipos informáticos operan en rangos de temperatura y humedad establecidos por los fabricantes. En los lugares donde estas condiciones no se cumplan, ya sea por las condiciones propias de la zona o porque se acumula una cantidad importante de equipos que en conjunto violan estos parámetros, se requiere contar con equipos de control ambiental especializados en equipo electrónico. Nuevamente, la continuidad del funcionamiento de la plataforma tecnológica depende de la continuidad de estos sistemas de control ambiental por lo que se requiere que los diseños garanticen esta operación constante.

- Sistemas de vigilancia y alarmas: Existen riesgos que pueden controlarse en forma automática mediante la implementación de sistemas de vigilancia y alarmas en áreas específicas. Entre estos riesgos podemos mencionar los de intrusión, calor, incendio e inundación. También se pueden implementar sistemas de circuito cerrado de televisión con la finalidad de que se pueda ver en forma remota lo que sucede en las áreas sensibles de la plataforma tecnológica.

- Control de Acceso: El acceso a las áreas sensibles, es decir, aquellas áreas donde se ubica equipo clave cuya falla podría provocar discontinuidad en los servicios, debe estar controlado. Este control puede realizarse en forma manual o electrónica mediante llavines electrónicos y tarjetas codificadas, sin embargo, solo el personal autorizado debe ingresar a estas áreas.

- Extinción de incendio: Un incendio puede provocar daños cuantiosos en muy poco tiempo al equipo electrónico. El fuego debe controlarse en el menor tiempo posible provocando un daño mínimo a los equipos. Los sistemas tradicionales de extinción de incendios resultan inadecuados por lo que debe optarse por un sistema de extinción de incendios especial para equipo electrónico.

- Mantenimiento de todos estos sistemas: Todos los sistemas que garantizan la seguridad física de la plataforma tecnológica requieren de un adecuado mantenimiento. Sin este mantenimiento los sistemas se deteriorarán incrementando el riesgo de falla. Es imprescindible no solo contar con estos sistemas sino que además se debe programar su sostenibilidad.

Refuerzo de la seguridad en los componentes de la plataforma tecnológica

Cada elemento que compone la plataforma tecnológica ofrece posibilidades para incrementar esta seguridad que no se deben desaprovechar. Estas medidas forman parte de los esfuerzos de bajo costo y mucho impacto en el nivel de seguridad informática de la organización. A modo de ejemplo se pueden citar los siguientes elementos y esfuerzos:

- Equipos servidores: los dispositivos en los que se ejecutan los servicios deben estar diseñados para tal fin. Dejando de lado las características de rendimiento que deben exhibir, deben contar con duplicidad en sus componentes críticos (procesadores, fuentes de poder, tarjetas de comunicación, etc., almacenamiento).

- Sistema operativo de los servidores: En primer lugar, el sistema operativo de los servidores controla el acceso a los recursos; como premisa se tiene que nadie debe tener acceso a un recurso que no necesita ni a privilegios de uso que no necesita. Pero además los sistemas operativos permiten la implementación de mecanismos adicionales que refuerzan la seguridad informática como pueden ser mecanismos de replicación de información o

incluso servicios. Deben conocerse e implementarse los mecanismos que mayor beneficio aporten.

- Hipervisores: La virtualización permite agregar una capa adicional de seguridad informática ya que facilita mecanismos que permiten incrementar la continuidad de los equipos virtuales y en dado caso reducen el tiempo de su recuperación. Pero además permite una mayor visibilidad en la administración de recursos lo que la faculta para realizar ajustes automáticos a la plataforma que mejoran su desempeño al tiempo que incrementan la continuidad de los servicios. También permiten la implementación de esquemas de intercomunicación de diferentes sitios con lo que se posibilita un mecanismo contingente en caso de una falla de nivel catastrófico de un sitio.

- Dispositivos de almacenamiento: El fin último de la seguridad informática es proteger la información de la organización. No es de sorprender que los dispositivos que almacenan esta información resulten cada vez más sofisticados y confiables, sin embargo, es importante conocer e implementar todas las facilidades que permitan estos equipos. Como ejemplos de estos mecanismos se pueden citar los diferentes arreglos de discos, la duplicidad de componentes y las facilidades para replicación de información.

- Bases de datos: Los motores de bases de datos funcionan como contenedores de la información de tal forma que no se puede acceder a esta sino es a través suyo. Para este fin estos productos implementan mecanismos que refuerzan la seguridad tales como administración de privilegios, filtrado de la información a través de vistas, integridad referencial, encripción tanto en el almacenamiento como en la comunicación, replicación y respaldo de la información. Deben habilitarse tantos mecanismos de seguridad como sea posible.

- Dispositivos de red: Los switches, enrutadores, puntos de acceso y otros dispositivos permiten el acceso a los equipos en los que se almacena la información. Esta función les permite también proveer mecanismos de seguridad que impiden que se utilicen equipos, protocolos o mecanismos para accesar información en forma indebida. Entre estos mecanismos podemos citar las VLANs en los switches, las listas de acceso en switches y enrutadores y hasta el propio diseño de la red en sus diferentes capas.

- Sistemas: Dependiendo de la forma en la que se desarrollen los sistemas informáticos de la organización el código fuente de estos puede constituirse en una debilidad o en una fortaleza. Existen múltiples ataques informáticos que aprovechan descuidos en los programas entre los que se pueden citar la inyección SQL, la ingeniería reversa y las puertas traseras. Es importante que los desarrolladores apliquen buenas prácticas de programación para que sus sistemas formen parte de los muros que protegen la información de la organización. Otro aspecto importante a tener en cuenta es la actualización constante del código; programas desactualizados utilizan componentes

desactualizados y potencialmente vulnerables por lo que el código debe estar en constante revisión con el fin de mantenerlo lo más actualizado posible.

- Equipos terminales del usuario: Los equipos terminales son un elemento que comúnmente se descuida y se constituye en punto de falla de la seguridad informática. Debe limitarse lo que el usuario pueda hacer con este de tal forma que un descuido de su parte no comprometa, en la medida de las posibilidades, la seguridad informática de la organización. Deben además deshabilitarse todos los elementos que no deban usarse ya que, en su configuración de fábrica podrían resultar de fácil acceso. También deben habilitarse mecanismos que mejoren la confiabilidad de los equipos, tal es el caso de los discos duros en espejo para evitar pérdidas de información en las computadoras. Es importante aclarar que en este aparte se incluyen también equipos como impresoras que se conectan a la red y que podrían tener habilitados protocolos o servicios que permitan la conexión a la red de un delincuente informático. En este sentido se recomienda estandarizar lo más posible y definir claramente la configuración que cada tipo de dispositivo deba tener.

- Mecanismos de respaldos: El buen uso de estos recursos reduce sustancialmente la pérdida de información. En la actualidad existen múltiples opciones que permiten llevar los tiempos de pérdida de información y de recuperación a valores muy razonables, sin embargo, mientras más eficientes sean estos mecanismos más costosos serán por lo que la organización deberá determinar cuál es el que puede costear y administrar el riesgo residual.

- Sistemas de monitoreo: La mayoría de los componentes críticos de la plataforma tecnológica de una organización son capaces de generar información que permite monitorear su funcionamiento en una o varias consolas lo que permite un manejo preventivo de las fallas o el dado caso una reacción más oportuna ante estas. El monitoreo de la plataforma se convierte por tanto en una herramienta indispensable.